CLMPTO TL 03/01/05

1. A method for preserving the integrity of a negotiation comprising the steps of:

5a) providing an architecture which includes a center A, and a plurality of users B.sub.1, B.sub.2,..., B.sub.n,

b) generating for each user B.sub.i an input X.sub.i,

c) inputting each user's input X.sub.i to the center A,

d) computing and publishing a function F(X.sub.1,X.sub.2,...,X.sub.n) by the center A based on the input messages it receives,

e) each user B.sub.i (1<= i<= n) communicating with the center A exclusively, and

f) publishing by center A additional information which lets each of the users verify that F was computed correctly, and preventing a coalition of any one subset of the users from learning (i) anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, and (ii) information about the inputs of other users.

2. The method of Claim 1 for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount he has to pay.

- - 3. (amended) The method according to [any one of claims 1 or 2] claim 1, for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount to be paid, and wherein the center only makes disclosure to the winning bidder, while all other bidders being able to verify that the auction was computed correctly, but do not learn any other information.

- - 4. (Amended) The method according to [any one of claims 1, 2 or 3] claim 1, for first price auctions, where the output of F is (B.sub.j, X.sub.j), where X.sub.j is greater or equal to any one X.sub.i for 1 <=i <=n.

- - 5. (Amended) The method according to [any one of claims 1, 2 or 3] claim 1, for second price auctions (Vickrey auctions), where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is greater or equal to any X.sub.i for 1 <=i <=n except for i=j1.

- - 6. (Amended) The method according to [any one of claims 1, 2 or 3] claim 1, for k-th price auctions, where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is the k-th largest among all inputs X.sub.i for 1 <=i <=n.

- - 7. (Amended) The method according to [any one of the preceding claims] claim 1 wherein the auction is a plural auction where there are a plurality of sellers.

- - 8. (Amended) The method according to [any one of the preceding claims] claim 1 wherein the auction is a generalized Vickrey auction.

- - 9. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of, computing the auction such that the auctioneer wants to buy an item and each of the bidders wants to sell this item, and wherein negative values of the inputs X.sub.i are possible.

- - 10. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of; computing the output of the auction such that the users learn, in addition, some statistic of the inputs, such as, the users can learn at least one of the average of the inputs, the variance of the inputs, or how many one inputs were in a certain range.

- - 11. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of computing the output of the function such that only the center learns the output of the function. or several of the users learn the output of the function, or all the users learn the output of the function.

- - 12. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of, computing the output of a mechanism, in particular, for one of Groves-Clark mechanisms, opinion polling and stable matching.

- - 13. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the steps of each user committing to the values of his input in a manner that the user cannot change it afterwards, but hiding the input value from the center,[.]at a specific stage, the users opening their commitments to their inputs and revealing their values to the center, which then computes the value of F in a manner the each of the users can verify that the values that were used as inputs for computing F were the values that were committed to by the users.

- - 14. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of implementing automated agents which participate in the auction which do not disclose to the auctioneer the limit price that they were given, until the end of the bidding period.

- - 15. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of computing a function where the center can generate a proof that it computed the correct output of the function.

- - 16. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of computing a function by N centers, such that only if K of the N centers collude they can learn information about the parties' inputs.

17. In a system that contains N parties, each having a private input, and a center adapted to compute a function F of said input; apparatus for computing said function F in said center, comprising:

a first program provided in the center that enables calculation of said function F;

circuitry for publishing said function F using the program while not revealing substantially any information about said input; and

a second program provided to the parties enabling each one of said parties to prove that said function F was calculated correctly.

18. In a system according to claim 17, wherein the second program precludes the learning of any information other than the function F was calculated correctly.

19. In a system according to claim 17, wherein the first program includes a construction of K garbled circuits for computing function F.

20. In a system according to claim 17, wherein said parties are bidders in an auction; said input are bids, said center is an auctioneer, said function F is the rule by which said auction is decided, whereby the auctioneer is capable of calculating the result of said auction without revealing any information about said bids, except for the identity of the winning party from among said parties, and the amount to pay.

21. In a system according to claim 20, wherein the function is determined utilizing a circuit of gates.

22. In a system according to claim 20, wherein the second program includes the capability of utilizing the circuit of gates to independently determine and verify that the computations of the center are correct.